IT-POL-006

Office of Information Technology Policy

Authentication

Purpose:
Access to data or resources in a computer system with the most basic level of security most often requires the user to identify himself and prove his identity. The user's identification (user-ID) tells the system who the user is and the user's password proves, or authenticates, the user's identity. Once the system knows who the user is, it can determine what data and resources the user can access.

Authentication focuses on something you know (passwords, PIN), something you have (digital tokens, smart cards) and something you are (biometrics). Any combination of these can be used to authenticate a user. Most computer systems rely on a user-ID and password for authentication. However, authentication can be much more secure when these methods are combined.

Information is a state asset that must be protected from unauthorized access, use, modification and destruction. The authentication process provides protection by controlling access to the assets of information technology systems. Authentication techniques permit validation of user's identities, hardware devices, and/or transmitted information.

Policy:
Agencies must use at least one of the following methods of authentication when accessing or utilizing state-owned or managed information technology systems.

- Passwords (IT-STD-009)
- Biometrics (IT-STD-010)
- Smart Cards (IT-STD-011)
- PKI (IT-STD-012)

Scope:
All agencies and entities under the authority of the Office of Information Technology pursuant to the provisions of R.S. 39:15.1, et seq. must comply with this policy.

Responsibilities:
Agencies are responsible for developing policies governing the authentication requirements detailed in this policy and its supporting technical standards.

Effective Date:

November 7, 2002
Reissued May 1, 2003 (revised scope statement)